IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
WESTERN DIVISION

Sandi Lazette,

Plaintiff

v.

Chris Kulmatycki, et al.

Defendant

Case No. 3:12CV2416

ORDER

This is a suit by Sandi Lazette, a former employee of the defendant Cellco Partnership, d/b/a Verizon Wireless (Verizon), and her supervisor, defendant Kulmatycki. The gravamen of the action is that, after plaintiff left Verizon's employee and returned her company-issued blackberry (which she used and refers to in her complaint as her "phone"), Kulmatycki, during the ensuing eighteen months, read without her knowledge or authorization 48,000 e-mails sent to plaintiff's personal g-mail account. In addition, plaintiff alleges Kulmatycki disclosed the contents of some of the e-mails to others.

This alleged conduct gives rise to five claims: 1) violation of the Stored Communications Act (SCA), 18 U.S.C. § 2701 *et. seq.*;[1] 2) violation of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III), 18 U.S.C. § 2510 *et seq;*[2] 3) Ohio common law invasion of

[1] 18 U.S.C. § 2707 provides a cause of action for violations of the SCA

[2] 18 U.S.C. § 2520 provides a cause of action for violations of Title III.

privacy/seclusion; 4) civil recover for violation of O.R.C. § 2913.04(B);[3] and 5) Ohio common law intentional infliction of emotional distress.

Pending is defendants' motion to dismiss. (Doc. 5). For the reasons that follow, I deny the motion in part and grant it in part.

Background

According to the complaint, the factual allegations of which I take as true, Verizon provided the blackberry for plaintiff's use. She was told that she could use the company-issued phone for personal e-mail. She had an account with g-mail, though she believed she had deleted that account from the phone before giving it to Kulmatycki in September, 2010. She understood that Verizon would "recycle" the phone for use by another employee.

In May, 2012, plaintiff learned that Kulmatycki, rather than deleting her g-mail account, had been accessing her g-mail account for a period of eighteen months. In addition, Kulmatycki, on information and belief, had disclosed the contents of the e-mails he had accessed.

Plaintiff neither consented to nor authorized Kulmatycki's surreptitious reading of her personal e-mails. His actions were within the scope and course of his employment with Verizon.

Once plaintiff was aware of Kulmatycki's actions, she changed her password to prevent further access. Before she did so, he had accessed 48,000 e-mails in plaintiff's g-mail account. Among the contents of the accessed e-mails were communications about plaintiff's family, career, financials, health, and other personal matters.

[3] O.R.C. §§ 2307.60, 2307.61 provide a cause of action for persons injured by another's felonious conduct.

Kulmatycki's conduct was knowing, intentional, willful, wanton, malicious, and fraudulent. He undertook his actions to benefit Verizon and further his own interests.[4]

Discussion

1. Stored Communications Act

Section 2701 of the SCA states in pertinent part:

> (a) Offense.--Except as provided in subsection (c) of this section whoever--
>
> > (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
> >
> > (2) intentionally exceeds an authorization to access that facility;
>
> and thereby obtains . . . access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.
>
> * * * * *
>
> (c) Exceptions.--Subsection (a) of this section does not apply with respect to conduct authorized--

[4] The defendants' motion to dismiss contains numerous factual allegations that more properly belong, if evidentiary support exists for them, and if there is no dispute about them, in a motion for summary judgment. I have ignored those allegations.

The motion to dismiss also suggests that the complaint generally fails to meet the *Twombly/Iqbal* pleading requirements. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). With one exception (relating to her intentional infliction of emotional distress claim), I disagree: plaintiff's complaint amply sets forth "enough facts to state [claims] to relief that [are] plausible on [their] face." *Twombly*, 550 U.S. at 570. Most simply, those well-plead facts allege Kulmatycki, without authorization, over an eighteen month period, accessed 48,000 e-mails in plaintiff's personal g-mail account. The fact that the complaint also – and properly so – recites or paraphrases statutory language does not somehow negate the plausibility of the claim she asserts under the statute, or take her complaint into *Twombly/Iqbal* territory. *Cf. Monson v. Whitby School, Inc.*, 2010 WL 3023873, *3 (D. Conn.) ("while Dr. Monson argues that Whitby's [SCA] allegation that her actions were 'unauthorized' is too 'conclusory' to state a viable claim, it is difficult to imagine how else Whitby could plead this necessary element." other than to assert actions were beyond scope of any authority).

> (1) by the person or entity providing a wire or electronic communications service; . . . .[5]

Section 2707 of the SCA provides in pertinent part:

> (a) Cause of action.– . . . [A]ny . . . person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

Relief available under this provision includes equitable relief, damages, and reasonable attorneys' fees and litigation costs. 18 U.S.C. § 2707(b).

The SCA incorporates the definition of "electronic storage" from Title III:

> (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

18 U.S.C. § 2510(17).

The defendants assert that Kulmatycki's opening and reading 48,000 of plaintiff's e-mails during an eighteen month period did not violate the SCA. In making this argument, they contend:

- The relief plaintiff seeks is not available because the legislative history shows that Congress aimed the SCA at "high-tech" criminals, such as computer hackers;
- Kulmatycki had authority to access plaintiff's e-mails;
- Kulmatycki's access did not occur *via* "a facility through which an electronic communication service is provided" other than the company owned blackberry;
- The e-mails were not in electronic storage when Kulmatycki read them;

[5] Sections 2703 (required disclosure of customer records), 2704 (backup storage), and 2518 (court orders for law enforcement electronic surveillance) are not applicable to what is presently at issue in this case.

- Verizon may be exempt from the SCA under § 2701(c)(1), which states that the person or entity providing an electronic communications service is exempt from the Act, because the complaint does not make clear that plaintiff's g-mail account was separate from her company account.[6]

a. Whether the SCA Applies

Defendants' reading of congressional intent and the case law with regard to whether the SCA prohibits unauthorized access to another person's g-mail account is not persuasive.

In support of their claim that Congress intended the SCA only to reach computer hackers, not someone who reads another person's e-mails without his or her knowledge, defendants cite *Int'l Ass'n of Machinists & Aero. Workers v. Werner-Matsuda*, 390 F. Supp. 2d 479, 495 (D. Md. 2005).

In that case, the court stated, "Federal courts interpreting these statutes have noted that their 'general purpose . . . was to create a cause of action against "computer hackers (*e.g.*, electronic trespassers). "'" (citing *Sherman & Co. v. Salton Maxim Housewares, Inc*. 94 F.Supp.2d 817, 820 (E.D.Mich.2000) (quoting *State Wide Photocopy Corp. v. Tokai Fin. Servs., Inc*., 909 F.Supp. 137, 145 (S.D.N.Y.1995)).

However, the case from which the court in *Machinists* derived its comment about the "general purpose" of the SCA, stated less restrictively: "generally, it appears that the ECPA was *primarily* designed to provide a cause of action against computer hackers, (*i.e*., electronic trespassers." *State Wide Photocopy, Corp. v. Tokai Financial Services, Inc*. 909 F.Supp. 137, 145 (S.D.N.Y. 1995) (emphasis supplied). "Primarily" does not mean "exclusively," despite defendants'

[6] I disagree with this contention. The complaint alleges the blackberry "contained both professional and personal email accounts." (Doc. 1, ¶ 3). It is clear from the complaint that plaintiff is talking about an account separate and distinct from her company-provided e-mail account.

assertion that Kulmatycki's conduct is outside the statute's scope because he was not a "hacker" in the conventional sense.[7]

Moreover, the case from which *Machinests* drew its specific language, *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F.Supp.2d 817, (E.D. Mich. 2000), also stated expressly, "The provisions of section 2701 of the Act apply to persons or entities in general and prohibit intentional accessing of electronic data without authorization or in excess of authorization." *See also Educational Testing Service v. Stanley H. Kaplan, Educational Center, Ltd.* 965 F.Supp. 731, 740 (D.Md. 1997) ("it appears evident that the sort of trespasses to which the Stored Communications Act applies are those in which the trespasser gains access to information to which he is not entitled to see"); *Thayer Corp. v. Reed*, 2011 WL 2682723, *7 (D.Me.) ("The statute does not limit liability to 'hackers.'").

The prohibitions of the SCA apply to the defendants.

b. Authority to Access Plaintiff's E-Mails

Defendants argue that Kulmatycki had authority to access plaintiff's g-mail account because: 1) he used a company-owned blackberry; 2) he did not access a "facility," as the statute uses that term; and 3) plaintiff authorized Kulmatycki's access because she had: a) not expressly told him not to read her e-mails; and b) implicitly consented to his access by not deleting her g-mail account.

i. Use of Company-Owned Device/Authorization

[7] The statement in *Wide Photo* was, moreover, dictum, as on the dissimilar facts of that case, the court did not depend on the statute's putative purposes – primary or otherwise – in dismissing the complaint. 909 F.Supp.2d at 146 ("State Wide's § 2702 claim is deficient in the same fashion as the § 2701 claim in failing to allege facts demonstrating that Tokai is covered by the described categories of prohibited actors or that State Wide is an aggrieved party within the meaning of the ECPA.").

Defendants claim that, because Kulmatycki indisputably had authority to use the blackberry on which others were sending e-mails to the plaintiff, he could use it to access those e-mails. In support of this contention, among the cases defendants cite are ones where one family member had accessed e-mails sent to another family member on a family computer. *White v. White*, 781 A.2d 85, 90–91 (N.J. Super. 2001); *State v. Poling*, 938 N.E.2d 1118, 1123 (Ohio App. 2010).

Those cases are readily distinguishable, as they involved joint users of a shared computer. Here, there never was joint use beteween plaintiff and Kulmatycki. Indeed, when Kulmatycki accessed e-mail sent to plaintiff, she was not able to use the blackberry to do likewise.

Other cases which the defendants cite are similarly inapposite. In *Lasco Foods, Inc. v. Hall and Shaw Sales, Marketing & Consulting, LLC*, 600 F.Supp.2d 1045, 1050 (E.D. Mo. 2000), the plaintiff expressly acknowledged the defendants, among whom were former company employees, had "virtually unrestricted access to its information." In other words, at the time the individual defendants had accessed the databases, the plaintiff knowingly, and with its approval, permitted them to do so.

Here, plaintiff neither knew nor approved of Kulmatycki's accessing her e-mails.[8]

---

[8] In *Lasco*, the plaintiff alleged the defendants had exceeded the scope of their authority when accessing company databases before leaving the plaintiff's employ. Rejecting this contention, the court noted the lack of factual support for that allegation in the complaint, and pointed out the plaintiff "has not identified any restricted information that Defendants supposedly accessed." 600 F.Supp.2d at 1050.

In this case, because I find that Kulmatycki lacked authority to access plaintiff's e-mails, at least to the extent that she had yet to open them, I need not reach the issue of whether Kulmatycki violated § 2701(a)(2), which makes liable one who "intentionally exceeds an authorization to access that facility". If, however, I were to find that somehow Kulmatycki had a right of access, he exceeded it by exercising that putative authority 48,000 times over an eighteen month period.

In *Sherman, supra*, after a former employee sued the defendant for breach of contract, the defendant company sought leave to counter-sue for a violation of the SCA. Its proposed counter-complaint asserted the former employee had used a computer and a company access code, which one of the company's customers had provided, to access sales data on the customer's database. The plaintiff thereafter provided that data to a competitor. 94 F.Supp.2d at 819.[9]

The circumstances in *Sherman* are likewise distinguishable. As in *Lasco,* the party in *Sherman* claiming a violation of § 2701 acknowledged in its complaint that the alleged miscreant had had authority to access the customer's vendor sales database. *Id.* The company's complaint was that its former employee had not had authority to view *its* sales information on that database and thereafter disclose that information. This contention, the court held, did not pass muster under either § 2701, prohibiting unauthorized access, or § 2702, prohibiting disclosure by service providers of the SCA. *Id.* at 820.

What matters here is that the aggrieved party in *Sherman*, unlike plaintiff here, acknowledged that the alleged intruder had had authority to access the database in the first instance.

To be sure, the court in *Sherman* noted that the former employee had not misused the company's password to access the customer's database. *Id.* at 821. Plaintiff's complaint does not allege password misuse as such.

[9] When the former employee had left the plaintiff's employ, it had instructed to customer to deny access to the customer's database. When the events giving rise to the complaint in *Sherman* occurred, the customer had not followed that instruction. 94 F.Supp.2d at 819.

While password misuse did not occur here, it does not matter. I find nothing in the statute or anywhere else that suggests – just as with defendants' claim that only hackers are liable – use of a password somehow is an element which a SCA plaintiff must prove.[10]

I conclude, accordingly, that the mere fact that Kulmatycki used a company-owned blackberry to access plaintiff's e-mails does not mean that he acted with authorization when he did so.

ii. Accessing a "Facility"

Section 2701(a)(1) prohibits "intentionally access[ing] without authorization a facility through which an electronic communication service is provided."

Defendants contend that Kulmatycki's conduct was lawful, because he used the blackberry to open and read plaintiff's e-mails. Their reasoning is that: 1) the blackberry was a "facility" within the meaning of § 2701(a)(1); 2) Kulmatycki was (indisputably) an authorized user of the blackberry; therefore, 3) the SCA permitted him to use such facility to do what he did. Accordingly, defendants conclude, plaintiff fails to state a claim under § 2701.

In support of their argument that the blackberry was a "facility," the defendants point to cases which have held that a personal computer qualifies as a "facility." *See Chance v. Ave. A, Inc.*, 165 F.Supp.2d 1153, 1161 (W.D.Wash. 2001); *In re Intuit Privacy Litig.*, 138 F.Supp.2d 1272, 1275 n. 3 (C.D.Cal. 2001); *Expert Janitorial, LLC v. Williams*, 2010 WL 908740, *5 (E.D.Tenn.).

[10] If Kulmatycki had authorization to access plaintiff's g-mail account, he necessarily would have had authorization to use her password. If allowed to enter, he was entitled to use the key. This circumstance distinguishes cases finding password misuse. *State Analysis, Inc. v. American Financial Services Assoc.*, 621 F.Supp.2d 309, 318 (E.D. Va. 2009); *Cardinal Health 414, Inc. v. Adams*, 582 F.Supp.2d 967, 977 (M.D.Tenn.,2008) (former employee who used former co-worker's log-in information "plainly violated the SCA as a matter of law.").

I disagree with defendants' reasoning and their contention that a personal computer, much less a blackberry, is a "facility" within § 2701(a)(1).

Neither Title III nor the SCA defines "facility." *Cornerstone Consultants, Inc. v. Production Input Solutions, L.L.C.,* 789 F.Supp. 2d 1029, 1050 (N.D. Iowa 2011); *Freedom Banc Mortg. Servs., Inc. v. O'Harra*, 2012 WL 3862209, *9 (S.D.Ohio).

The recent decision in *In re iPhone Application Litigation*, 844 F.Supp.2d 1040 (N.D. Cal. 2012), makes clear that a cell phone is not a "facility." After emphasizing, "the computer systems of an email provider, a bulletin board system, or an ISP are uncontroversial examples of facilities that provide electronic communications services to multiple users," the court also acknowledged, "less consensus surrounds the question presented here: whether an individual's computer, laptop, or mobile device fits the statutory definition of a "facility through which an electronic communication service is provided." *Id.* at 1058.

The court in *iPhone* then turned its attention to the cases, noted above, which have equated a personal computer to be a § 2701(a)(1) "facility." Those cases, in the court's view, "provide little analysis on this point of law, instead assuming plaintiff's position to be true due to lack of argument and then ultimately ruling on other grounds." *Id*. at 1058-59.

Finding these cases, as I do, unhelpful, the court in *iPhone* looked to and followed the decision in *Crowley v. CyberSource Corp*., 166 F.Supp.2d 1263, 1271 (N.D. Cal. 2001). In *Crowley* the court pointed out that, if the computer which is accessed and the computer through which acces occurs are both "facilities," it would certainly "seem odd that the provider of a communication service could grant access to one's home computer to third parties, but that would be the result of Crowley's argument." Taking this circuitous route, the court observed, "would equate a user with

a provider and, thus, ignore language in § 2701(c) that treats users and providers as different." *Id*. at 1270. A user of a service, as Kulmatycki was when he accessed plaintiff's e-mails, is not also the provider of those same e-mails.

Thus, the better, more sensible, and harmonious reading of the SCA is that a personal computer, and, *ergo*, a blackberry or cell phone, is not a "facility" within § 2701(a)(1).

Several other courts agree that devices with which a user accesses electronic communications are not "facilities." *Garcia v. City of Laredo*, 702 F.3d 788, 792-93 (5th Cir. 2012); *Cornerstone Consultants, supra*, 789 F.Supp. 2d at 1050 (pertinent "facility" through which an electronic communication service is provided is e-mail server); *Freedom Banc, supra*, 2012 WL 3862209, *8 ("the relevant 'facilities' that the SCA is designed to protect are not computers that enable the use of an electronic communication service, but instead are facilities that are operated by electronic communication service providers and used to store and maintain electronic storage.").

Instead, the "electronic communications service" resided in the g-mail server, not on the blackberry, and the g-mail server, not the blackberry, was the "facility."

iii. Plaintiff did not Authorize Access to her E-Mails

Plaintiff deleted the e-mails she had received before leaving Verizon. But she did not also close her g-mail account, though she believed she had done so. Her failure to be more careful, defendants contend, deprives her of any claim under the SCA.

Defendants correctly contend that the essence of plaintiff's complaint is that Kulmatycki accessed her e-mails without her consent. According to them, the plaintiff negligently and/or implicitly consented to his doing so when she returned the blackberry without having ensured that she had deleted her g-mail account.

Defendants also point out that plaintiff's complaint does not allege that Kulmatycki took any affirmative steps to cause the device to receive e-mails. Nothing in the SCA requires one who accesses a service provider without authorization also to have done something to the equipment to facilitate his access.[11] To the extent that plaintiff has to prove the Kulmatycki did anything "affirmative," she has done so *via* her contention that he read her e-mails. Doing so required opening the e-mails, which was an affirmative act on his part.

Turning to the substance of defendants' contentions, defendants, in effect, contend that plaintiff's negligence left her e-mail door open for Kulmatycki to enter and roam around in for as long and as much as he desired.

This is an unacceptable reading of § 2701(a)(1), which prohibits "access without authorization," and of the private party consent surveillance provision, 18 U.S.C. § 2511(2)(d).[12] To be sure, consent under this provision need not be explicit, it can, as defendants allege, also be implied. *Williams v. Poulos*, 11 F.3d 271, 281 (1st Cir.1993). Negligence is, however, not the same as approval, much less authorization. There is a difference between someone who fails to leave the door locked when going out and one who leaves it open knowing someone be stopping by.

---

[11] I also reject any suggestion that plaintiff has to prove that she affirmatively instructed Kulmatycki and Verizon that they were not permitted to access her g-mail account. To be sure, the court in *Sherman*, *supra*, found no SCA violation because, as to the former employee, there was never a "clear[ ] and [ ] explicit restriction on access." 94 F.Supp.2d at 821. I find nothing in the statute that requires this sort of prophylaxis as a prerequisite to imposing liability on an unknown and unexpected electronic intruder. At most, if at all, the absence of such directive might be a consideration when determining damages from the intrusion.

[12] Section 2518(2)(d) provides, "[i]t shall not be unlawful under this chapter for a person . . . to intercept a[n] . . . electronic communication . . . where one of the parties to the communication has given prior consent to such interception."

Whether viewed through the lens of negligence or even of implied consent, there is no merit to defendants' attempt to shift the focus from Kulmatycki's actions to plaintiff's passive and ignorant failure to make certain that the blackberry could not access her future e-mail. On this issue, a case involving a claim of implied consent under 18 U.S.C. § 2511(2)(d), *Griggs-Ryan v. Smith*, 904 F.2d 112 (1st Cir. 1990), is instructive:

> [I]mplied [consent] is "consent in fact" which is inferred "from surrounding circumstances indicating that the [party] *knowingly agreed to the surveillance*." Thus, implied consent-or the absence of it-may be deduced from "the circumstances prevailing" in a given situation. The circumstances relevant to an implication of consent will vary from case to case, but the compendium will ordinarily include language or acts which tend to prove (or disprove) that a party knows of, or assents to, encroachments on the routine expectation that conversations are private. And the ultimate determination must proceed in light of the prophylactic purpose of Title III-a purpose which suggests that consent should not casually be inferred.

Id. at 116-17. (citations omitted) (emphasis supplied). *Accord, Williams, supra*, 11 F.3d at 281.

Indeed, even "knowledge of the capability of monitoring alone cannot be considered implied consent." *Deal v. Spears*, 980 F.2d 1153, 1157 (8th Cir.1992). In that case the court held an employee did not impliedly consent to monitoring of her phone calls when her employer only told her that it might monitor phone calls. *Id.* In this case, where plaintiff believed she had eliminated her g-mail account from the blackberry, she was unaware of the possibility that others might access her future e-mails from that account.

What it takes to find implied consent shows clearly that plaintiff here did give such consent. Thus, in *U.S. v. Workman*, 80 F.3d 688, 693 (2d Cir.1996), the court found an inmate had impliedly consented where a notice by the telephone and prison handbook told him calls would be monitored. Similarly, in *Griggs–Ryan, supra*, 904 F.2d at 118, the plaintiff had been told several times that monitoring of phone calls would occur. In *Shefts v. Petrakis*, 758 F.Supp.2d 620, 631 (C.D. Ill.

2010), the court found implied consent where the employee manual informed him text messages would be logged.

Consent to access otherwise private electronic communications can, under § 2511(2)(d), constitute authorization to read those communications. Even when a party gives such consent, it is limited by its own terms. An inmate who knows his phone conversations with a friend might be monitored does not expose his communications with his attorney to a jailer's ear. Here, even if plaintiff were aware that her e-mails might be monitored, any such implied consent that the law might perceive in that knowledge would not be unlimited. Random monitoring is one thing; reading everything is another.

c. Electronic Storage

The defendants claim that the the complaint fails to allege sufficient facts to establish that the e-mails Kulmatycki accessed were in "electronic storage" when he accessed them. As previously noted, the SCA incorporates the definition of "electronic storage" in § 2510(17) of Title III: "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for the purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

The defendants argue, and several courts have agreed, that only e-mails awaiting opening by the intended recipient are within this definition. *In re DoubleClick, Inc. Privacy Litig*., 154 F.Supp.2d 497, 511–12 (S.D.N.Y. 2001); *Fraser v. Nationwide Mut. Ins. Co.*, 135 F.Supp.2d 623, 635–36 (E.D.Pa.2001); *U.S. v. Weaver*, 636 F.Supp.2d 769, 771 (C.D.Ill. 2009); *Hilderman v. Enea TekSci, Inc*. 551 F.Supp.2d 1183, 1205 (S.D.Cal. 2008) ("courts have construed subsection (A) as

applying to e-mail messages stored on an ISP's server pending delivery to the recipient, but not e-mail messages remaining on an ISP's server after delivery."; *Jennings v. Jennings*, 736 S.E.2d 242, 245 (S.C. 2012).[13] E-mails which an intended recipient has opened may, when not deleted, be "stored," in common parlance. But in light of the restriction of "storage" in § 2510(17)(B) solely for "backup protection," e-mails which the intended recipient has opened, but not deleted (and thus which remain available for later re-opening) are not being kept "for the purposes of backup protection." *Jennings*, *supra*, 736 S.E.2d at 245.

Thus, plaintiff cannot prevail to the extent that she seeks to recover based on a claim that Kulmatycki violated the SCA when he accessed e-mails which she had opened but not deleted. Such e-mails were not in "backup" status as § 2510(17)(B) uses that term or "electronic storage" as § 2701(a) uses that term.

With regard to e-mails which plaintiff had yet to open before Kulmatycki did so, defendants argue that her allegations about her unopened e-mails being in electronic storage fail the *Twombly/Iqbal* test. This is so, because plaintiff does not specify which of the 48,000 e-mails which Kulmatycki allegedly accessed were awaiting opening by plaintiff.

---

[13] Courts taking a contrary view, and concluding that § 2510(17)(B) "backup storage" includes opened, undeleted e-mails are in a minority and involve, in my view, a strained reading of that provision. *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1071 (9th Cir. 2004) ("prior access is irrelevant to whether the [e-mails] at issue were in electronic storage."). *See generally* Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L.Rev. 1208, 1217 (2004) ("*Theofel* is quite implausible and hard to square with the statutory test."). Moreover, that the Sixth Circuit would follow *Theofil* and extend SCA protection to opened but undeleted e-mails is doubtful. *See U.S. v. Warshak*, 631 F.3d 266, 291 (6th Cir. 2010) (quoting Kerr, *supra*).

Given the volume of e-mails which plaintiff alleges Kulmatycki opened, I believe that I can draw a fair and plausible inference that Kulmatycki opened some of those e-mails before plaintiff did, and thus, in doing so, violated § 2701(a).[14]

Plaintiff's complaint adequately alleges that Kulmatycki violated § 2701(a) when he opened e-mails before she did.

In light of the foregoing, I overrule defendants' complaint to the extent that it seeks dismissal *in toto* of plaintiff's SCA claim. I grant it, however, to the extent that plaintiff seeks to recover for his opening of e-mails which she had opened before he did.

d. Verizon's Vicarious Liability

Plaintiff alleges, and defendants acknowledge, that Kulmatycki's actions were within the scope of his employment by Verizon and in furtherance of its interest. Defendants seek dismissal of Verizon on the basis that it may be exempt from liability under§ 2701(c)(1). That provision states that an entity providing an electronic communications service is exempt from the Act.

---

[14] At this stage of this case, it appears that the extent of Kulmatycki's violation is a matter of damages, rather than of liability *ab initio*. While the jury cannot speculate as to damages, it can consider circumstantial proof as to such issues as how often and when plaintiff and Kulmatycki accessed her g-mail account. Or, it may be possible (though I simply don't know whether it is), for forensic analysis to ascertain when each of them accessed a message, and thereby, possibly, arrive at a very precise figure with regard to which e-mails plaintiff had and had not opened before Kulmatycki did.

These are matters for the forthcoming stages of this case. For now, I only conclude that plaintiff has stated a plausible, albeit circumstantial, claim that Kulmatycki opened some e-mails before she did. After all, 48,000 e-mails during an eighteen-month period is a daily average of something less than 100. That Kulmatycki opened some of plaintiff's e-mails before she did is likely enough for now. On the other hand, it is highly unlikely that he opened, on average, 100 of plaintiff's e-mails every day before she did.

In support of this supposition, defendants contend that the complaint does not make clear whether plaintiff's g-mail account was separate from the account Verizon provided for her work-related use. If so, then, according to defendants, Verizon would have become a provider of electronic communication services and within the exemption of § 2701(c)(1).

Once again, defendants look outside the four corners of plaintiff's complaint for assistance. All that plaintiff had to assert was that she had a g-mail account and Kulmatycki accessed her e-mails without authorization. She has done so.

It is up to defendants to develop the evidentiary and legal basis for their challenge, which is in the nature of an affirmative defense. A plaintiff does not bear the burden of anticipating defenses and pleading over them in order to avoid Rule 12(b) dismissal. *Veney v. Hogan*, 70 F.3d 917, 921(6th Cir. 1995) ("the plaintiff need not fully anticipate the defense in the complaint"), *overruled in part on other grounds*, *Goad v. Mitchell*, 297 F.3d 497 (6th Cir. 2002).

Plaintiff has, in any event, asserted, and defendants have admitted that Kulmatycki was acting within the scope of his employment and in furtherance of Verizon's interests when he accessed plaintiff's e-mails. Defendants' motion does not challenge plaintiff's actual theory of liability – namely, that Verizon is vicariously liable for Kulmatycki's actions, much less shown that conventional master-servant liability law does not apply.

I overrule defendants' motion to dismiss Verizon.

2. Title III

Plaintiff claims that Kulmatycki's conduct included not only accessing her stored electronic communications, but disclosing those communications to others. This, she contends, gives rise to a cause of action under 18 U.S.C. § 2520, the civil liability provision of Title III.

Defendants claim that plaintiff has failed to state a cause of action under § 2520. They base their contention on two provisions of Title III, 18 U.S.C. § 2510(4) and § 2510(5), found in the statute's definition section.

Section 2510(4) defines "intercept" to mean "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.

Section 2510(5) defines "electronic, mechanical, or other device" to mean "any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than" certain exceptions not applicable here.

The term "interception" in § 2510(4) does not encompass electronic communications stored, as the e-mails here were, for the intended recipient's retrieval on her own computer. *E.g.*, *Fraser v. Nationwide Mutual Insurance Co.*, 352 F.3d 107, 113 (3d Cir.2003); *Steve Jackson Games, Inc. v. Secret Service*, 36 F.3d 457 (5th Cir.1994); *Konop v. Hawaiian Airlines, Inc*., 302 F.3d 868 (9th Cir.2002); *United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir.2003).

In response, plaintiff points to the Seventh Circuit's decision in *U.S. v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010). In that case, the defendant installed a "rule" on his supervisor's computer. The device caused the defendant's computer to receive the e-mail whenever the supervisor's e-mail service provider sent a message to the supervisor's computer. *Id*. at 703. Thus, the defendant acquired the e-mail from the service provider directly and concurrently, not by later accessing the service provider's computer. Receipt of the e-mail by each within "no more than an eyeblink" constituted interception by the defendant under § 2510(5). *Id.* at 706.

Here, in contrast, Kulmatycki went to the server's computer, where plaintiff's g-mail account was to be found. By then, g-mail had already sent the message to plaintiff's computer.

Kulmatycki did not, therefore, "intercept" plaintiff's e-mail, and Title III does not cover his actions.

That being so, the defendants' motion to dismiss plaintiff's Title III claim is well-taken.[15]

3. Invasion of Privacy:
Intrusion into Seclusion

Plaintiff claims that Kulmatycki's actions give rise to an Ohio common-law tort claim for invasion of privacy/ intrusion into seclusion. With regard to such claim, the court in *Moore v. Univ. Hospitals of Cleveland Medical Center*, 2011 WL 5554272, *4 (N.D.Ohio) stated:

> Citing Section 652B of the Restatement of Torts 2d, the Ohio Supreme Court [has] said, "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." *Sustin v. Fee*, 69 Ohio St.2d 143, 431 N.E.2d 992, 993–94 (Ohio 1982). The key language is that the affairs or concerns must be private to rise to be actionable as an invasion of privacy. *See Olson v. Holland Computers, Inc*., 2007 WL 2694202, at *4 (Ohio Ct.App.2007) ("In order to establish a wrongful intrusion into private activities, a plaintiff must show that he or she had a reasonable expectation of privacy in the area allegedly intruded."

In *Moore*, the court granted summary judgment to the defendant as to plaintiff's claim that it had "broken into" the e–mail account which the defendant provided. The court found the plaintiff had failed to allege evidence to support his claim. In addition, it also found plaintiff had not established, in the face of defense evidence of warnings about monitoring, that he had had a reasonable expectation of privacy. *Id., *4.*

[15] It is not necessary to consider the parties' arguments about Kulmatycki's use of a "device" under the statute, as that is a moot issue in light of the lack of interception in this case.

Although this decision properly states the applicable law as to the elements of plaintiff's claim, defendants' reliance on it to justify dismissal is misplaced. This is so, because, as plaintiff points out, I cannot consider the contents of defendants' employee handbook, which it attached an exhibit to the motion to dismiss. Considering that exhibit, much less whether it constituted a defense to plaintiff's claim would, at this stage, be entirely premature.

Moreover, it would be one-sided. Courts in Ohio apply a totality of the circumstances test to determine whether an individual has a reasonable expectation of privacy. *See, e.g.*, *State v. Corbin*, 194 Ohio App.3d 720, 727 (2011); *see also Savoy v. U.S.*, 604 F.3d 929, 935 (6th Cir. 2010) (applying state totality of circumstances law in case involving state tort claims of intrusion *via* videotaping).

Many factors can affect whether plaintiff's expectations that no one would intrude into her e-mail account, particularly in light of her unawareness of Kulmatycki's ability to do so. Indeed, the precise terms of the warning matter. With regard to what one might expect from a warning of the possibility of occasional, random monitoring is one thing, total absorption is another. Here there are, in any event, several preliminary issues that have yet to be addressed. Among these, aside from the content of the warning, are just what did Kulmatycki do, when did he do it, what were his motives, when might plaintiff have become aware of his intrusions, and what and from whom had she learned about using her company blackberry for a personal e-mail account. These and other factors may have a bearing on the reasonableness of what plaintiff might reasonably have expected when she returned her blackberry.

Otherwise, with regard to the elements of this tort, I find plaintiff's claim survives the pending motion. Her e-mails were highly personal and private. A reasonable jury could find

Kulmatycki's reading of tens of thousands of such private communications, if proven to have occurred, "highly offensive."

I find that plaintiff has stated a viable claim for privacy/intrusion into seclusion. *See Eysoldt v. ProScan Imaging*, 194 Ohio App.3d 630, 639 (Ohio App. 2011) (evidence sufficient that defendant turned plaintiff's e-mail accounts over to third party who could read them).

4. Claim Under O.R.C. § 2913.04

Plaintiff asserts a claim under O.R.C. §§ 2307.60, .61 , which permit a person injured by another's criminal conduct to recover against the perpetrator of the crime. In this case, O.R.C. § 2913.04(B) defines the crime on which plaintiff bases her claim:

> No person, in any manner and by any means, including, but not limited to, computer hacking, shall knowingly gain access to, attempt to gain access to, or cause access to be gained to any computer, computer system, computer network, cable service, cable system, telecommunications device, telecommunications service, or information service without the consent of, or beyond the scope of express or implied consent of, the owner of the computer, computer system, computer network, cable service, cable system, telecommunications device, telecommunications service, or information service or other person authorized to give consent.

The defendants assert two ground for dismissal: plaintiff did not own the blackberry, so that they were entitled to use it to gain access to her g-mail account, and, in any event, the statutory purpose is to deter computer hacking.

Defendants misread these very broad and inclusive provisions of this remedial statute. It says nothing about who owns the means of intrusion: indeed, it is as likely that an intruder would use his or her own device as he or she would use someone else's device to gain access to that person's computer or computer-based information.

Second, and even more completely off the mark, the defendants claim that this is simply an anti-hacking statute, and has nothing to do with a finding out something that he or she has no

business or right to find out. By its own terms, the statute states, "including but not limited to, computer hacking." In plain English, "including but not limited to" is not a term of limitation, but one of limitless expansion.

In any event, cases applying O.R.C. § 2913.04(B) have encompassed a broad range of misconduct. Appellate courts have upheld convictions of defendants who have: misused a work computer to access a work-related database with a personal, non-work related motive, *State v. Claborn*, 2012 WL 1078930, *2 (Ohio App.), entered computer network and caused damage, *State v. Holt*, 2011 WL 1204330, *1 (Ohio App.), locked the victims out of their internet accounts, used the victims' names to send vulgar messages to others, and sent vulgar messages about the victims to others, *State v. Cline*, 2008 WL 1759091, *1 (Ohio App.), continued using using a cable box after disconnection without provider's consent, *State v. Sullivan*, 2003 WL 22510808, *4 (Ohio App.), improperly accessed law enforcement criminal records database, *State v. Moning*, 2002 WL 31127751, *1 (Ohio App.), used another's phone to make long distance calls, *State v. McNichols*, 139 Ohio App.3d 252, *254 (Ohio App. 2000), improperly accessed Law Enforcement Automated Data system, *State v. Giannini*, 1998 WL 886961, *1 (Ohio App.), committed telephone toll fraud, *State v. Redd*, 1994 WL 178451, *1 (Ohio App.), and installed password protected software on workplace computer without authorization. *State v. Johnson*, 1992 WL 25312, *1 (Ohio App.).

The plaintiff has stated a claim under O.R.C. §§ 2307.60, .61 and § 2913.04(B).

5. Intentional Infliction of Emotional Distress

Plaintiff's final claim is for intentional infliction of emotional distress.

The elements of such claim are:

> (1) the defendant intended to cause emotional distress, or knew or should have known that his actions would result in serious emotional distress; (2) the defendant's

> conduct was so extreme and outrageous that it went beyond all possible bounds of decency and can be considered completely intolerable in a civilized community; (3) the defendant's actions proximately caused psychological injury to the plaintiff; and (4) the plaintiff suffered serious mental anguish of a nature no reasonable person could be expected to endure.

Yeager v. Local Union 20, 6 Ohio St.3d 369 Yeager v. Local Union 20 (1983) (syllabus).

The defendants argue that plaintiff's allegations relating to mental anguish are insufficient. Even aside from *Twombly/Iqbal*, the pleading requirement with regard to the injury are quite high: namely, that the defendant's actions "caused psychological injury," and "plaintiff suffered serious mental anguish."

Plaintiff's complaint makes no allegation of psychological injury. More importantly, her claim of having suffered severe mental anguish is entirely conclusory. That being so, I conclude that it is insufficient under the *Twombley/Iqbal* standard. *See Foxx v. Healix Infusion Therapy, Inc.,* 2013 WL 791188, *7 (E.D. Tenn.) ("plaintiff does not sufficiently allege a serious mental injury as required for the claim. Plaintiff merely alleges in conclusory fashion that her termination 'would cause the Plaintiff severe emotional distress' and that she suffered 'humiliation and embarrassment, and emotional distress.'").

I shall, however, grant plaintiff four weeks from the date of entry of this order to file an amended complaint in which she states that she either has been undergoing treatment for psychic injuries, suffered specific and prolonged psychic and/or psychic-related consequences, or both. *See, e.g., Buckman-Peirson v. Brannon*, 159 Ohio App.3d 12, 21 (2004). If plaintiff fails to file an amended complaint stating a plausible claim for intentional infliction of emotional injuries, this count shall be dismissed with prejudice.

Conclusion

For the foregoing reasons, it is

ORDERED THAT:

1. Defendants' motion to dismiss plaintiff's claims under 18 U.S.C. § 2520 and claims under 18 U.S.C. § 2701 to the extent she seeks § 2701 recovery for accessing opened, but undeleted e-mail, be, and the same hereby is granted;

2. Defendants' motion to dismiss plaintiff's other claim for violation of the Stored Communications Act and her state law claims for civil recovery for criminal acts, and invasion of privacy-seclusion be, and the same hereby is overruled;

3. Defendants' motion to dismiss plaintiff's claim for intentional infliction of emotional distress be, and the same hereby is denied, subject to plaintiff's filing within four weeks of the date of th is order of an amended complaint as required herein; if plaintiff fails to files an amended complaint within that time, defendants' motion to dismiss this count shall be granted.

The Clerk shall forthwith set a status/scheduling conference.

So ordered.

/s/ James G.Carr
Sr. U.S. District Judge